REMARKS

In response to the Final Office Action mailed December 26, 2007, Applicant respectfully requests reconsideration. Claims 1-23 were previously pending in this application. By this amendment, Claims 1, 8, 15 18, 20 have been amended. As a result, claims 1-23 are pending for examination with claims 1, 8, 18 and 20 being independent claims. No new matter has been added.

INTERVIEW SUMMARY

Applicants thank the Examiner for the courtesy of a telephone interview on February 6, 2008. During the interview, the Balissat and Hur references were discussed in conjunction with the independent claims. The amendments and remarks herein may serve as a further summary of the interview.

Claim Rejections - 35 U.S.C. § 112

Claim 18 is rejected under 35 U.S.C. §112as being indefinite. The Office Action highlights the phrase: "the public key-pair of the DH key." Applicants propose an amendment to this phrase to address the issue noted by the Examiner. Applicants respectfully request that the amendment be entered and the rejection be withdrawn.

Art-Based Rejections

Each of the claims pending in the application is rejected based on U.S. Patent 7,188,365 to Balissat et al., (Balissat) either alone or in combination with U.S. Patent 7,181,620 to Hur (Hur). Applicants respectfully disagree with the rejection.

A summary of the disclosure of the present application and a discussion of the Balissat reference were provided in conjunction with the amendment filed October 2, 2007. Applicants also pointed out at least one limitation of each of the claims that is not met by Balissat. For brevity, that summary and a full listing of limitations not met by the reference is not repeated here. Rather, Applicants respond to specific issues on the Office Action.

Hur is newly cited in the outstanding Office Action. However, this reference does not change the validity of any of the points previously made. Hur does not describe limitations of the claims that are not met by Balissat. Rather, Hur relates to distribution of keys to newly deployed network devices (Col. 1, lines 8-14). Accordingly, the reference is not cited to show using a key, exchanged through an Internet key exchange (IKE), to authenticate the identity of a device, as described in the present application.

Applicants address certain points raised in the section of the Office Action entitled "Response to Arguments." First, Applicants disagree with the Examiner's statement: "Examiner finds the number of messages used for authentication is irrelevant because the claimed invention does not limit to a single transmission of data, message, payload, or packet to authenticate the identity of the responder or the initiator." Though the claim does not expressly recite a number of messages, Applicants respectfully submit that the number of messages in Balissat is nonetheless an indication that the reference is not describing a method as claimed. As recited in claim 1, and as amended for greater clarity, a public key communicated as part of an Internet key exchange negotiation "is a claim on the identity of at lease one of" the devices engaging in the key exchange and may be used to authenticate the identity of the device. The fact that the reference uses additional messages, following the IKE negotiation, to exchange information to authenticate the identity after Diffie-Hellman keys have been exchanged indicates that the reference is not using a key exchanged during the IKE negotiation to authenticate the identity of the device and is not performing the method of claim 1.

The Office Action also states: "For it is the same key-pair that is used between the first device (initiator) and the second device (responder) used in forwarding (encrypted) packets that is associated with authentication of the device by the establishment of security association SA (Col. 6, lines 60-64)." Applicants respectfully disagree that the cited passage of the reference describes authentication of a device, or in the words of claim 1, a key used to "authenticate the identity of" another device. A security association may be used to determine that specific messages were generated by the same device that participated in a key exchange. However,

knowing that a message was generated by the same device that provided a key is not the same as authenticating the identity of the device. Thus, the cited passage of Balissat does not teach the limitations of claim 1.

On page 5, the Office Action cites passages of Balissat, such as column 2, lines 43-62 and column 7, lines 55-63. These passages use the term security association and, in some places, the term "authenticate." However, these passages do not describe authenticating an identity. Applicants respectfully submit that in the context of the reference, the meaning of the term "authenticate" is revealed at column 2, lines 60-62. That passage indicates that the term "authenticate" means that a user that sent a transmission is identified. In other words, the sender of a message is related to a party who provided a key. The actual identity of the party is not verified. Thus, claim 1 recites a method of establishing secure communications that uses a public key in a fashion not described in Balissat. For at least this reason, the rejection of claim 1 should be withdrawn.

Claims that depend from claim 1 further emphasize the distinction. For example, dependent claims 2 through 5 recite that the key, acting as a claim on the identity of one device, is previously known to the other device. Regardless of how the term "authenticate" is used in the reference, this limitation is not met by the reference which performs authentication based on keys exchanged during or after IKE negotiation.

Independent claim 8 also recites a key used as "a claim on the identity" of another device in a fashion that is not described in Balissat. Dependent claims 9-12 recite limitations that further distinguish the reference. These claims also recite that a public key acting as a claim on the identity of one device was previously known to the other device.

Independent claim 15 has been amended to incorporate a limitation that emphasizes differences with Balissat. As amended, claim 15 recites both that "at least one key of the DH-pair being made available . . . prior to initiating communication according to the IKE protocol," and that "a static Diffie-Hellman key-pair authenticates a device."

Claim 18, as amended, makes clear that a public key obtained from portable media "is used to verify the identity" of a device, and that this identification occurs "prior to forming a security association." Accordingly, claim 18 makes clear that forming a security association as in Balissat does not meet all limitations of the claim.

Independent claim 20 similarly recites that a public key "is a claim on the identity of" another device. As should be apparent from the foregoing, such limitations distinguish Balissat.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: March 26, 2008

Respectfully submitted,

By:
Edmund J. Walsh
Registration No.: 32,950
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000